

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America
 v.

Case No. **1:25-mj-371**

Carl David Innmon

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 3/11/2025 in the county of Travis in the
Western District of Texas, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Section 2252(a)(4) (B)	Possession of Child Pornography
18 U.S. Code § 2252 (a)(2)	Receives Child Pornography

This criminal complaint is based on these facts:

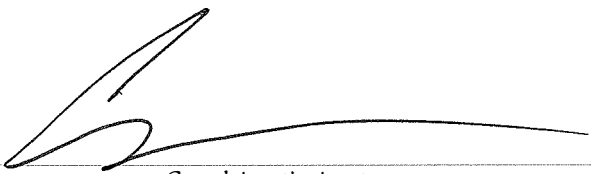
See attached affidavit

☒ Continued on the attached sheet.

☐ Sworn to before me and signed in my presence.
☒ Sworn to telephonically and signed electronically at 8:45 a.m.

Date: 04/01/2025

City and state: Austin, Texas


Complainant's signature

SA Craig Swantner, TFO / FBI

Printed name and title


Judge's signature

Susan Hightower, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Craig Swantner, being duly sworn, depose and say that:

Your affiant is Special Agent (SA) Craig Swantner, certified and licensed as a master peace officer by the Texas Commission on Law Enforcement and commissioned by the Texas Department of Public Safety (DPS). Your affiant completed the 26-week DPS Law Enforcement Academy in March of 2008, after which followed his assignment as a State Trooper in the Texas Highway Patrol Division. Affiant is currently an SA in the Criminal Investigations Division (CID) assigned to DPS Headquarters Computer Information Technology and Electronic Crimes (CITEC) unit. Affiant is also assigned as a Task Force Officer to the FBI Cyber Taskforce in Austin. Affiant conducts and assists with cybercrime investigations, cryptocurrency, fraud, crimes involving a computer nexus, digital forensics, and investigations involving possession of child pornography, possession of lewd visual material, child sexual abuse material, online solicitation of a minor, and other crimes of child sexual exploitation. In this capacity, affiant has attended multiple digital forensic, cyber investigations, social media, interviewing, fraud, child abuse and exploitation, and cryptocurrency training courses, including The International Association of Investigative Specialists (IACIS), National Computer Forensic Institute (NCFI), Professional Law Enforcement Training (PLET), Cellebrite, National White Collar Crime Center (NW3C), National Domestic Communications Assistance Center (NDCAC) and Internet Crimes Against Children (ICAC). Affiant has been involved in numerous search warrant executions involving internet crimes.

This affidavit is being submitted in support of a Criminal Complaint for **CARL DAVID INNMON, DOB: [REDACTED]**.

The factual information supplied in this affidavit is based upon your Affiant's own involvement in the investigation of this matter, as well as information provided by other law enforcement officers as outlined below in this affidavit. The Affiant has set forth facts that he believes establishes probable cause to believe that **CARL DAVID INNMON** has violated the provisions of Title 18, U.S.C. Sections 2252(a)(4)(B) Possession of Child Pornography and Title 18, U.S.C. Sections 2252A(a)(2), Receipt of Child Pornography.

Peer-to-peer file sharing (P2P) is a method of communication available to internet users using special software that allows people to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the internet and is often free to download. The software is designed to allow users to trade digital files through a worldwide network formed by linking computers directly instead of through a central server. Computers that are part of this network are referred to as "peers" or "clients." There are different

software applications that can be used to access these networks, but these applications operate in essentially the same manner. This software is used exclusively for the purpose of sharing digital files over the internet.

The BitTorrent network is a popular and publicly available P2P file-sharing network. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the internet, the user is able to download files from other users on the network and share files from their device with other BitTorrent users. A peer/ client computer can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different torrent network programs, examples of which include the BitTorrent client program, the uTorrent client program, the Gnutella client program, and the BitComet client program, among others.

During the installation of typical BitTorrent network client program, various settings are established that configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/ clients on the BitTorrent network, these other peers/ clients on the network can download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. The reassembly of pieces of files is accomplished using hash values, which are described more fully below. Once a user has completed the download of an entire file or files, the user can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files. A host computer that has all the pieces of a file available for uploading to the internet is termed a "seeder." Using the BitTorrent protocol, several basic computers, such as home computers, can replace large servers while efficiently distributing files to many recipients.

Files or sets of files are shared on the BitTorrent network using "Torrents." A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but rather contain information about the file(s) to be shared. This information includes the "info hash," which is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent. The term SHA-1 is a shorthand term for the hash value calculated by the Secure Hash Algorithm. The Secure Hash Algorithm (SHA-1) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA-1 hash functions and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA-1 signatures provide a certainty exceeding 99.99%, that two or more files with the same SHA-1 signature are identical copies of the same file regardless of their file names.

The data contained in the Torrent information includes the SHA-1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This "info hash" uniquely identifies the Torrent file on the BitTorrent network.

To locate Torrent files of interest and download the files that they describe, a typical user will use keyword searches on Torrent-indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent-indexing websites do not actually host the content (files) described in and by the Torrent files, only the Torrent files themselves or a link that contains that SHA-1 hash value of the Torrent or the files being shared. Once a Torrent file is located on the website that meets a user's keyword search criteria, the user will download the Torrent file to their computer. The BitTorrent network client program on the user's computer will then process that Torrent file to help facilitate finding other peers/ clients on the network that have all or part of the file(s) referenced in the Torrent file.

For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a Torrent-indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). Based on the results of the keyword search, the user would then select a Torrent of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the Torrent file. Using BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the Torrent file and that these file(s) are available for sharing. The user can then download the file(s) directly from the computer(s) sharing them. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file(s) with other users on the network. The downloaded file(s) are then stored in an area or folder previously designated by the user's computer or on an external storage media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user.

An IP address (Internet Protocol address) is a unique numerical identifier assigned to each device connected to a computer network, such as the internet. It helps devices communicate with each other by identifying and locating them on the network. There are two main types of IP addresses:

1. **IPv4:** This is the most common type, using a 32-bit format, expressed as four sets of numbers (each between 0 and 255) separated by periods (e.g., 192.168.1.1).
2. **IPv6:** This newer version uses a 128-bit format, allowing for a much larger number of unique addresses and is expressed in eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

An IP address can be either **static** (fixed) or **dynamic** (changing).

Law enforcement can search the BitTorrent network to locate individuals sharing child pornography images, which have been previously identified as such based on their SHA-1 values. Law enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/ clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

During the query and/ or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/ or downloading a file from. This information includes (1) the suspect client's IP address; (2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and (3) the BitTorrent network client program and version being used by the suspect computer. Law enforcement can then log this information.

The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. The ICAC Task Force Program uses law enforcement tools to track IP addresses sus (based on SHA1 values and file names) of trading child pornography. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/ or distributing child pornography, some of whom were also involved in contact sexual offenses against child victims.

On or about May 19, 2023, DPS CID began an undercover operation to identify persons using the BitTorrent P2P network on the internet to receive, traffic in, share and/ or distribute images and videos depicting child pornography and child sexual abuse material. Agents participating in this investigation have received training in the operation and use of the BitTorrent P2P network, as well as certain law enforcement techniques used to investigate users on this network.

SA Camarillo began investigating host computers located in Texas that were actively sharing child pornography on the BitTorrent network. Using specialized law enforcement software, SA Camarillo identified a host computer using Internet Protocol (IP) address 70.123.8.55 actively sharing Files of Interest (FOI), which are digital video and/ or image files that depict child pornography and/or child erotica, identified through keyword searches or info hash value searches for files containing known child pornography images and videos. This is accomplished through a law enforcement software client that searches for FOI for child pornography and child erotica.

Your affiant works with SA Oscar Camarillo daily and knows SA Camarillo to be an honest and credible law enforcement officer. SA Camarillo is also assigned to CITEC with your affiant and is on the same squad. Your affiant has worked on numerous investigations with SA Camarillo. SA Camarillo initiated and was the lead SA of this investigation.

SA Camarillo is a certified peace officer commissioned by DPS. SA Camarillo has been a peace officer for over 6 years and has been assigned to CITEC since November 2022. SA Camarillo has experience investigating violations of the Texas Penal Code, including but not limited to the procurement and execution of search warrants, pen registers, and precision location services orders, as well as interviewing and working with victims and witnesses.

SA Camarillo has personal experience and training in the interdiction of illegal contraband and has personally arrested and filed numerous criminal cases in State Court. SA Camarillo has

participated in and assisted with investigations (including joint investigations with other law enforcement agencies) of criminal statutes involving child exploitation laws, including receiving, manufacturing, collecting, and distributing child pornography, which involved surveillance, overt and covert operations, writing and serving search warrants, the arrest of individuals, and interviewing and interrogation. SA Camarillo has completed training in Fourth Amendment Search and Seizure and Interdiction for the Protection of Children.

SA Camarillo has experience viewing numerous photos and videos depicting child pornography (as defined in 18 U.S.C. §2256 and in Articles 43.25 and 43.26 of the Texas Penal Code). These examples, also referred to as Child Sexual Abuse Material or Child Sexual Assault Material (CSAM), were of known child victims identified and confirmed by law enforcement.

SA Camarillo has specialized training in the areas of criminal investigations, interview and interrogation, child abuse and exploitation, Internet Crimes Against Children (ICAC) investigations, and BitTorrent Investigations provided by federal, state, and local agencies and has specialized training in the seizure and analysis of computer equipment. SA Camarillo has experience with the execution of search warrants involving internet crimes.

Your affiant learned the following about this investigation from SA Oscar Camarillo:

1. A review of the image and video portions downloaded to the law enforcement computer from the host computer connected to the Internet through IP address 70.123.8.55 established that within the media and video files that the host computer shared or attempted to share, there are depictions of multiple minor children under the age of eighteen engaged in sexually explicit conduct, constituting child pornography pursuant to Texas Penal Code 43.26, Promotion or Possession of Child Pornography and 18 U.S.C. §§2252(a)(4)(B) and 2256.
2. On Sunday, December 29, 2024, between 1528 hours and 1559 hours, a download was successfully completed of 1 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.
3. On Monday, December 30, 2024, between 1043 hours and 1127 hours, a download was successfully completed of 4 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.
4. On Monday, December 30, 2024, between 1851 hours and 2025 hours, a download was successfully completed of 13 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

5. On Tuesday, December 31, 2024, between 2223 hours and 2224 hours, a download was successfully completed of 75 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.
6. Between Tuesday, January 14, 2025, at 2341 hours and Wednesday, January 15, 2025, at 0231 hours, a download was successfully completed of 25 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.
7. On Wednesday, January 15, 2025, between 0004 hours and 0229 hours, a download was successfully completed of 4 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.
8. On Wednesday, January 15, 2025, between 0132 hours and 0302 hours, a download was successfully completed of 4 file(s) that the device at IP address 70.123.8.55 was making available. The device at IP Address 70.123.8.55 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.
9. The device using IP address 70.123.8.55 downloaded a total of one hundred and twenty-six (126) files that depict an image of a child engaging in sexual conduct or sexual performance.
10. SA Camarillo viewed all of the files downloaded, and below is a description of three:
 - a) Folder Name – “3 yo Disneyland”
 - a. This folder contains several images in sequence depicting a nude infant between the ages of 0 and 2. Images “3todl-015” to “3todl-34” depict the same nude female infant child lying on her back. There is an erect adult male penis penetrating the child’s anus. The adult male then uses his index finger and thumb to force open the infant’s vagina while he continues to penetrate the child’s anus. The adult male appears to be pinning the infant down on top of what appears to be a diaper.
 - b) Folder Name – “PTHC CP JulyJailbait club”
 - a. This folder contains a video named “1”. The video depicts a female child between the ages of 5-7 lying fully clothed on her back. The video is taken from the point of view angle. The adult male recording the video zooms in to the vaginal area of the female and rubs his erect penis on the child’s underwear near her vagina. The adult male then moved the child’s underwear to the side, exposing the child’s vagina. The adult male then inserts his finger in the child’s vagina. The adult male then takes the female’s clothes off, fully exposing the child. The male continues to run his fingers on the child’s anus and vagina.

- c) Folder Name- "Red 2"
- a. This folder contains several images in sequence depicting a nude female child between the ages of 4 and 5. The child is lying on her back naked. Images "red2-001" to "red2-005" depict the child exposing her vagina to the camera. An adult male then inserts his erect penis inside of the child's vagina.
11. SA Camarillo served a subpoena to Charter Communications for IP address 70.123.8.55 on February 19, 2025. Charter Communications responded on February 25, 2025, and identified the IP address to be registered to CARL INNMON at [REDACTED], **Austin, Texas 787[REDACTED]**. Your Affiant conducted surveillance at [REDACTED], **Austin, Texas 787[REDACTED]** and identified four (4) vehicles in the driveway registered to [REDACTED] Innmon. The vehicles include a white Tesla displaying Texas license plate SYJ [REDACTED], a gray Toyota SUV displaying Texas license plate CZ7 [REDACTED], a white Toyota passenger car displaying Texas license plate JLK [REDACTED], and a dark gray Toyota Camry displaying Texas license plate MHB [REDACTED].
 12. On March 5, 2025, SA Camarillo observed Carl Innmon drive and operate the dark Gray Toyota Carmy. Carl Innmon drove to Baranoff Elementary School. A Texas Work Force Commission check revealed that Carl Inmon is employed by Austin ISD as a 5th-grade ESL teacher.
 13. Based on the investigation conducted, on March 10, 2025, District Judge Muller with the 403rd District Court, Travis County signed a search warrant for [REDACTED], **Austin, Texas 787[REDACTED]**.
 14. The search warrant was executed by SA Camarillo on March 11, 2025. SA Camarillo spoke to Carl Innmon, DOB [REDACTED], who was located inside of [REDACTED], **Austin, Texas 787[REDACTED]**.
 15. During the execution of the search warrant your affiant served on the entry team and was assigned evidence custodian after securing the residence. Your affiant was responsible for securing and logging the evidence seized from INNMON.
 16. SA Camarillo advised Carl Innmon that he was not under arrest. INNMON stated to SA Camarillo that INNMON did download child pornography. INNMON stated to SA Camarillo that INNMON was in possession of child pornography located on a Lenovo Laptop S/N PF3S14KV.
 17. In addition, INNMON stated that INNMON owned and had access to INNMON's cellphone described as an Apple iPhone 11 Model A2111 S/N DNPZR16DN734, a Seagate Portable Hard Drive S/N NAEB1NCR, and a Lenovo Laptop S/N PF3S14KV.
 18. Based on the above, on March 11, 2025, District Judge Muller with the 403rd District Court, Travis County, Texas signed a search warrant for the following devices:

- Apple iPhone, M/N A2111, S/N DNPZR16DN734
- Lenovo Laptop S/N PF3S14KV
- Seagate Portable Hard Drive S/N NAEB1NCR

19. The search warrant for the devices was executed by SA Camarillo and by Digital Forensic Analyst (DFA) Alex Bundy.

20. Alex Bundy, Digital Forensic Analyst, is currently employed with the Texas Department of Public Safety in the CITEC Unit, since July 2022. Alex Bundy graduated with a Bachelor of Science in Criminal Justice and obtained a master's degree in Homeland Security. Alex Bundy worked for the Austin Police Department Crime Scene Unit from 2017-2022 and received 400 hours of crime scene training. In 2022, Alex Bundy obtained two certifications from Cellebrite (Cellebrite Certified Operator and Cellebrite Certified Physical Analyst). Analyst Bundy completed an 8 week in house training through the Texas Department of Public Safety CITEC Unit. Analyst Bundy completed a 36-hour SANS Defense Initiative of Smartphone Forensic Analysis in Depth course in December 2023. In May 2024, Analyst Bundy obtained a certification through Magnet Axiom as a Certified Forensic Examiner. In June 2023, obtained a certification from SANS Institute for GIAC Advanced Smartphone Forensics. Analyst Bundy has specialized training in the areas of child abuse, child exploitation, and BitTorrent investigations, by state and local agencies; also has specialized training in the analysis of computer equipment. Analyst Bundy has previously been involved in the execution of search warrants involving internet crimes. Analyst Bundy has been required to observe and review numerous examples of child pornography (as defined in 18 U.S.C. §2256 and as articles 43.25 and 43.26 of the Texas Penal Code define visual material and sexual conduct) in all forms of media, including computer media. Many if the numerous examples of child pornography, also referred to as Child Sexual Abuse Material or Child Sexual Assault Material (CSAM), were of known child victims identified and confirmed by law enforcement.

21. On the Lenovo Laptop, there was a total of eighty-one (81) files flagged as Category 1-Child Abuse and sixteen thousand and sixty-nine (16,069) files flagged as Category 2-Child Exploitation. On the external Seagate Hard drive, there was a total of twenty-eight thousand and two hundred and fifty-six (28,256) files that were flagged as Category 1- Child Abuse. There was a total of three hundred and twenty-one thousand and four hundred and seventy-two (321,472) files that were flagged as Category 2- Child Exploitation. DFA Bundy reviewed the files manually and confirmed all files were CSAM. The following three (3) videos were located on the Seagate Portable Hard Drive S/N NAEB1NCR:

- Filename: 2010 Kait 5Yo-Fuck & Suck, cum on face.avi

One video that was three minutes (3) and thirty-three (33) seconds in length. The video showed a female child between the ages of four to six (4-6) years old. The female child was lying on her back and exposing her vaginal area. The child's legs were bent at the knee and pulled towards her chest. The child's fingers were penetrating her vagina repeatedly. An adult hand was shown rubbing and forcing the child's vagina open. The camera would zoom into the hole of the child's

vagina. The adult's index finger was shown penetrating the child's vagina repeatedly. An adult erect penis was then shown being forced into the child's vagina. The adult hand would push the erect penis into the child's vagina, repeatedly. The female child was shown holding the erect penis with both of her hands. The next clip showed the same female child placing her mouth on the adult's erect penis. The female child then looks at the camera and wipes her mouth. The next clip showed the same female child lying on her back with an adult erect penis ejaculating onto the child's face and chest area.

- Filename: 2010 Kait 5Yo- Fuck 2

One video that was one minute (1) in length. The video showed a female child from the waist down, who appeared to be four to six (4-6) years old. An adult erect penis was shown penetrating the child's vagina, repeatedly.

- Filename: 2010 Kait 5Yo-Fucking Compilation

One video was three minutes (3) and forty-five (45) seconds in length. The video showed a female child between the ages of four and six (4-6) years old. The video showed a female child lying on her back while being penetrated by an adult erect penis, repeatedly. The next clip showed the same naked female child on top of the adult male lying on his back. The female child was shown penetrating the erect penis with her vagina, repeatedly. The video zoomed into the child's vagina and a white clear substance was oozing out. The next clip showed the female child lying on her back with her legs bent at the knee. The child's knees were pulled into her chest, and she was urinating.

22. The videos described above are a videotape or film that visually depicts conduct constituting the penetration of the anus or sexual organ of a child defined by TXPC 22.011 (a)(2).
23. Based on the above Magistrate Alfred Jenkins III, issued an arrest warrant for Carl Innmon on March 12, 2025, for Possession of Pornography >= 50 Depic or Video - First Degree Felony TXPC 43.26 (d)(2)(B). Judge Jenkins III is a magistrate judge for Travis County, Texas.
24. In addition to the known CSAM images, INNMON was in possession of Artificial Intelligence (AI) generated child pornography. SA Camarillo observed on INNMON's devices that INNMON had a large quantity of real images depicting students in a classroom. On INNMON's devices, those same images were placed in an AI generator, and the students were de-clothed.
25. SA Camarillo, with the assistance of Austin Independent School District (AISD) and AISD Police, was able to positively identify the students and their ages depicted in the images.

26. For the purpose of this arrest warrant, the students identified in the manufactured child pornography are going to be referred to as Child 1 and Child 2. Child 1 and Child 2 were identified to be students at Baranoff Elementary School, where Carl Innmon was a teacher.
27. Child 1 was identified to be born in 2013 and ten (10) years of age at the time the photo was taken. Below is a description of the original picture taken of Child 1 in the classroom by Carl Innmon:

Filename: IMG_8978.JPG

On 12/10/2024 at 9:00AM (UTC-6), one photograph was created with an Apple iPhone 11. The picture showed Child 1 sitting on top of her shoes and legs bent at the knee, who is identified as a child in Carl Innmon's class at the time the picture was taken. The female child's hair was pulled back into a ponytail. The female child was wearing a sweatshirt with the distinctive lettering. The female child was wearing blue colored jeans. In the background of the photograph there was a distinctive colored and logoed bag on the floor.

28. Below is the description of the AI-generated child pornography image that was generated with Child 1's face on it.

Filename: image (6).webp

On 3/10/2025 at 10:11PM(UTC-6), a photograph was created from the original photograph of Child Victim #1, that was described above. The photograph was cropped to only show from her nose to her waist. The female child had the same facial features as the original photograph of Child Victim #1. The device user had altered the photograph to depict Child Victim #1 exposing her breast and stomach area. The same distinctive colored and logoed bag with the word was on the floor in the background of the photograph.

29. In addition to the AI-generated child pornography. Carl Innmon was in possession of AI-generated images depicting Child 1 and Child 2 in a lewd exhibition.

30. Below is the description of Child 1 depicted in a lewd exhibition defined under section 43.262 on the TXPC.

Filename: image (5).webp

On 3/10/2025 at 10:09PM(UTC-6), a photograph was created from the original photograph of Child Victim #1, which was described above. The photograph was cropped to only show from her nose to her waist. The female child had the same facial features as the original photograph. The device user had altered the picture to show Child Victim #1 wearing a white colored lace bra and underwear. The female child had a white colored collar along with long sleeves covering both arms. The same distinctive colored and logoed bag was again on the

floor in the background of the photograph. The second confirmed student female was the same from the original photograph, who was in the bottom right corner.

31. Child 2 was identified to be born in 2014 and ten (10) years of age at the time the photo was taken. Below is a description of the original picture taken of Child 2 in the classroom by Carl Innmon:

Filename: IMG_9138.JPG

On 1/17/2025 at 8:07AM(UTC-6), one photograph was created with an Apple iPhone 11. The photograph showed Child 2 sitting on the floor wearing distinctive colored pants and a distinctive colored and logoed sweatshirt. Child 2 was positively identified by AISD and AISD Police as a student in Carl Innmon's class during the 2024-2025 school year.

32. Below is the description of Child 2 in a lewd exhibition defined under section 43.262 on the TXPC.

Filename: 789759768.webp

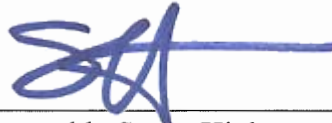
On 2/20/2025 at 8:53PM(UTC-6), the image showed Child 2 wearing a distinctive colored sweatshirt and black colored spandex. The child's legs were exposed and Child 2 had mid-calf length white colored socks on. This picture was recreated from the original student photograph and depicted Child 2 on a beach setting in a lewd manner.

Based on the aforementioned facts, your Affiant respectfully submits that there is probable cause to believe that from on or about March 11, 2025, within the Western District of Texas, **CARL DAVID INNMON**, committed the following offenses: Possession of Child Pornography, in violation of, 18 U.S.C. Section 2252(a)(4)(B); and Received Child Pornography, in violation of 18 U.S.C. Section 2252(a)(2).



Craig Swantner, DPS Special Agent
Task Force Officer / FBI

Sworn to and subscribed before me this 1st day of April, 2025.



The Honorable Susan Hightower
United States Magistrate Judge
Western District of Texas